HOPSWORKS

SOVEREIGN AI BLUE PRINT

Global Survey Insights on Building Trustworthy AI Systems

<JULY 2025>

> Sovereign AI is where an organization is capable of building and operating their own AI systems, ensuring data security and compliance with local regulations within the organization’s boundaries.
>
> - *Source: Hopsworks Dictionary*

Table of Contents

This report presents a **practical blueprint** for organizations aiming to implement **Sovereign AI responsibly**. As artificial intelligence becomes increasingly integrated into core operations, the need for **secure, compliant, and self-governed AI systems** is more urgent now.

The sections ahead explore key practices, frameworks, and sector-specific considerations that empower enterprises to deploy AI confidently in today's regulatory and technological landscape.

Executive Summary

In Q2 2025, we surveyed 100+ practitioners actually building AI systems; not consultants, not analysts, people writing code and managing infrastructure. Here's what we found:

Nearly half (46%) of organizations trying to implement AI don't have the adequate infrastructure.

Three Reasons Driving Adoption:

- Data privacy requirements (74%)
- Regulatory compliance (58%)
- Risk reduction (48%)

Three Gaps Consistently Present:

- Lack of expertise (63% for processes, 53% for infrastructure)
- Cost (50-70% depending on scope)
- System complexity (46-61% across different areas)

Geographic spread: 69% Europe (mostly Northern/Western), 12% Americas, rest distributed globally. Company sizes ranged from startups to enterprises.

Key Finding: Organizations are surprisingly pragmatic. 57% use hybrid approaches (build + buy), and 77% start with LLMs because they deliver quick wins. But production use cases remain traditional: automation (45%) and predictive analytics (52%).

This report aims to provide a realistic baseline for your AI strategy.

Executive Summary

Respondents were drawn from a broad spectrum of regions, industries, and organizational roles, underscoring the global and cross-sector relevance of Sovereign AI. This wide-ranging representation reinforces the understanding that Sovereign AI is no longer a theoretical or regulatory construct, but rather a strategic priority embraced by a growing and diverse set of stakeholders.

In this section, we describe the nature of the respondents, who they are, where they come from, and what roles they occupy within their organizations.

Current AI Talent Landscape

As the focus on adopting AI technologies intensifies, the experience level of the talent driving these initiatives plays a pivotal role in determining the maturity and compliance of implementation strategies. Understanding the professional backgrounds of those working in AI today provides insight into the field's current capacity to meet the demands of Sovereign AI, regulatory alignment, and ethical data governance. The figure below shows the current level of experience in the AI field and highlights opportunities for growth and skill development to advance responsible AI innovation.

In this survey, 82% of respondents have under 10 years of experience in AI. While unsurprising, this highlights a critical need for targeted training in data sovereignty and responsible AI governance.

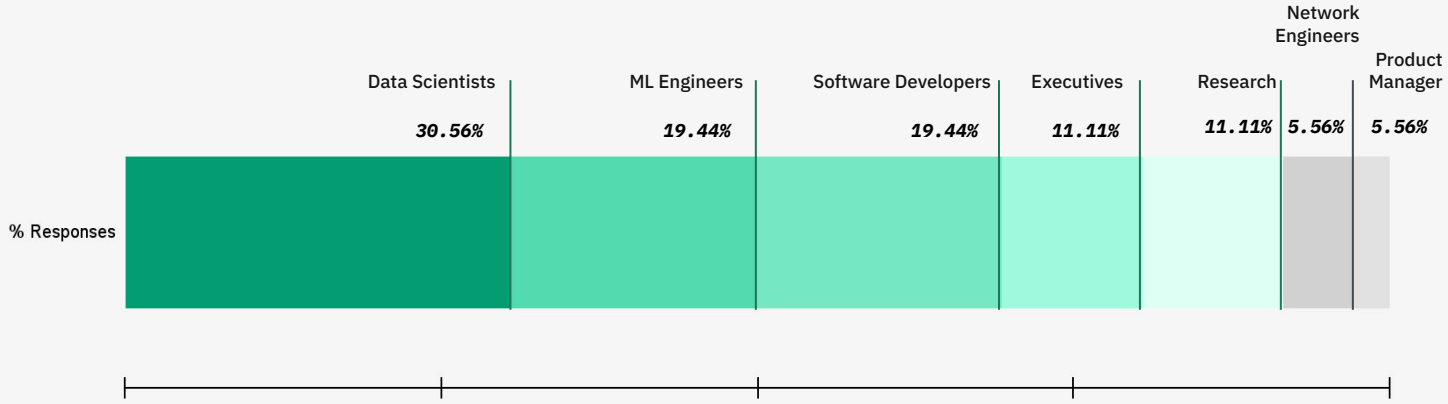
Executive Summary

Role Distribution

The Participants' Expertise Tells a More Nuanced Story than the Experience Data Alone Suggests.

From C-level executives and AI strategists to technical practitioners and compliance leaders, participants reflect a rich mix of perspectives and responsibilities. Their insights offer a multidimensional view of how Sovereign AI is being approached across different organizational contexts and maturity levels.

Participants came from a Broad Range of Roles,



The respondents included a diverse range of experts such as *Data Scientists, Senior Data Scientist – ML & Python, Chief Data Scientists, Senior Data Science Architects, Data Analytics Managers, Senior ML Engineers, ML Engineers, AI Governance Researcher, Software Engineers, Software Engineer – Interoperability, Product Owners/Full Stack Developers, Full Stack LLM Developer – AI and Big Data, Web Developer, Research Scientist – Machine Learning, PhD Candidate – Computer Vision, Multimodal AI, Professor – AI, ML, NLP, Project Managers, Data Engineers, and Network Engineers.*

AI's future is being written by people who've already solved hard problems. These aren't just AI enthusiasts: they are technical architects who've built systems that work; they are researchers in adjacent fields; and they are leaders who've successfully deployed complex technologies across entire organizations.

This isn't accidental. AI requires exactly this blend: deep technical knowledge and experience turning game changing ideas into value creating business systems.

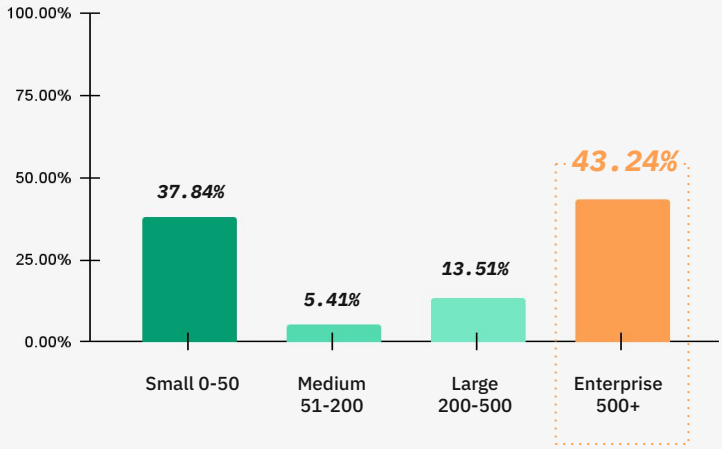
Executive Summary

Industry Distribution

Organizational Landscape by Size

Organization size drives everything from AI budgets to implementation timelines, making it crucial to understand who's actually driving adoption. The survey reveals a telling split: enterprise firms lead slightly, but smaller companies aren't far behind.

This mix reflects a dynamic landscape where data innovation isn't confined to big tech or large corporations, it's also thriving in nimble startups and growing companies across the industry spectrum.

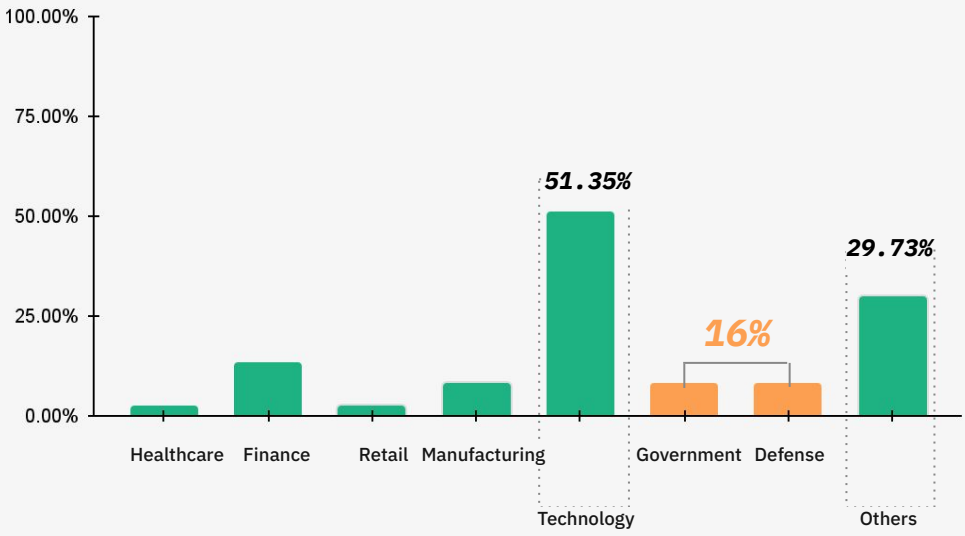


Enterprises are often better positioned to implement governance frameworks, likely due to their resources and ability to rapidly meet evolving requirements.

Industry Breakdown of Respondents

This section highlights the industries where respondents' organizations operate, offering insight into how different sectors are engaging with data and AI.

29.73% fall under 'Other' industries, including niche areas like Energy, Education, Gaming, Research, Plant Breeding, and Electricity, showing growing interest in Sovereign AI.

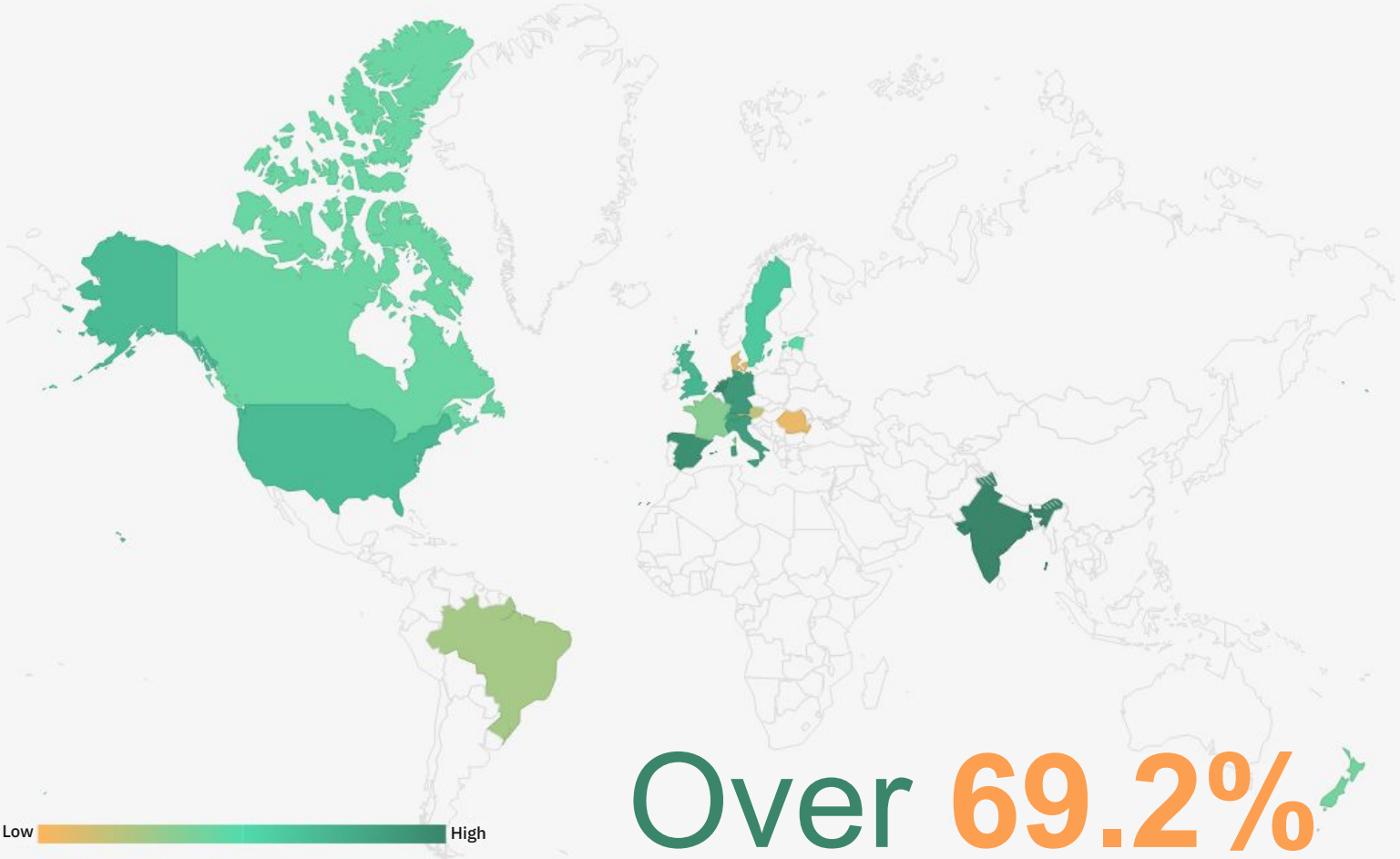


16%

of combined responses are from government and defense sectors demonstrating a growing reliance on AI to modernize public service delivery, improve national security, & inform strategic decision-making.

Executive Summary

Geographic Distribution: Global



Over **69.2%** of respondents

are based in Europe, where data sovereignty has emerged as a central concern amid increasingly strict regulatory frameworks.

Executive Summary

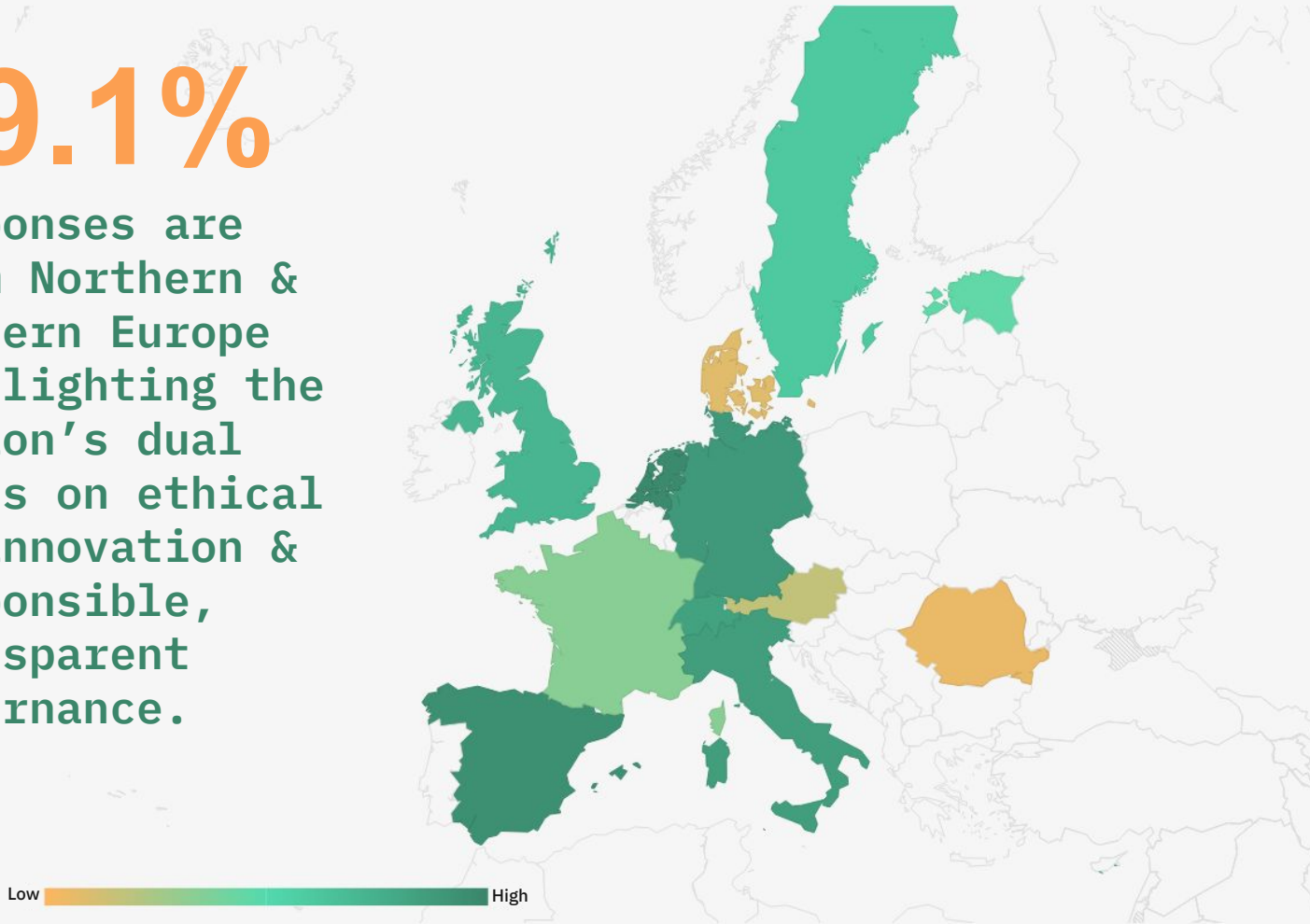
Geographic Distribution: Europe

Europe's dominance in the data underscores its ***strategic leadership*** in advancing AI under a ***regulated, ethical, and sovereign framework***, driven by ***policy foresight*** and a strong institutional ecosystem committed to ***transparency and accountability***.

With frameworks like the ***EU AI Act*** and ***GDPR***, European nations are prioritizing ***digital sovereignty*** and ***accountability*** at both national and continental levels. Their focus on ***transparent AI models***, ***secure local data usage***, and ***consistent EU-wide standards*** showcases how Europe is operationalizing ***Sovereign AI principles*** across ***policy, research, and implementation***.

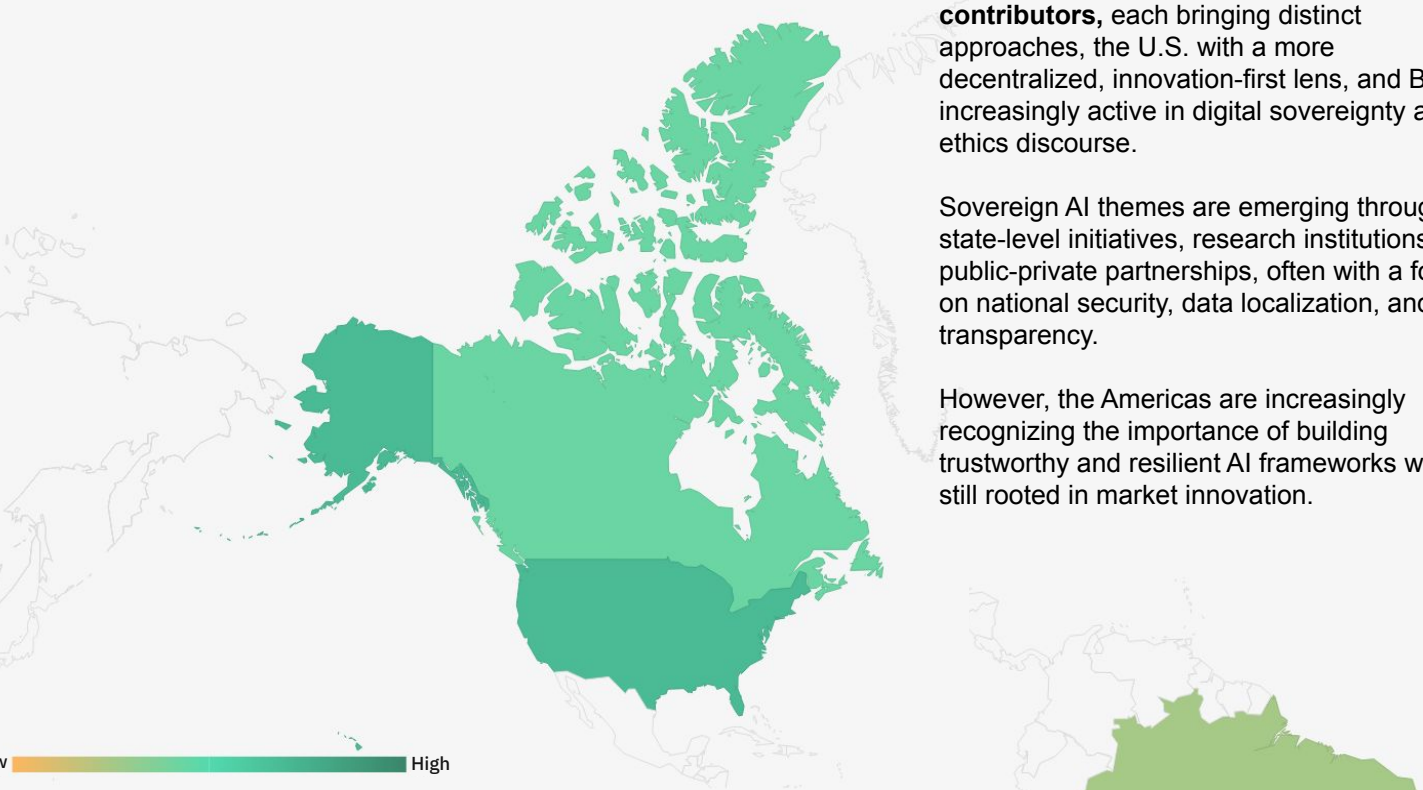
79.1%

responses are from Northern & Western Europe highlighting the region's dual focus on ethical AI innovation & responsible, transparent governance.



Executive Summary

Geographic Distribution: The Americas



The United States and Brazil appear as key contributors, each bringing distinct approaches, the U.S. with a more decentralized, innovation-first lens, and Brazil increasingly active in digital sovereignty and AI ethics discourse.

Sovereign AI themes are emerging through state-level initiatives, research institutions, and public-private partnerships, often with a focus on national security, data localization, and AI transparency.

However, the Americas are increasingly recognizing the importance of building trustworthy and resilient AI frameworks while still rooted in market innovation.

11.6% of responses originated from North and South America, highlighting a region balancing technological advancement with early-stage regulatory and sovereignty considerations.

1 Section:

AI Applications & Challenges

Section Overview

This section explores the various approaches organizations are taking to build and deploy AI within the context of a Sovereign AI framework, emphasizing key aspects such as model development, underlying infrastructure, and governance practices.

We found out that organizations face a complex set of strategic decisions:

1. **Developing AI in-house,**
2. **Leveraging external partners,**
3. **Adopting hybrid models.**

These three approaches represent different paths and choices towards sovereign, and ML systems capabilities. Developing AI in-house means building custom models and infrastructure from the ground up, offering the benefit of great control but at the cost of significant technical expertise and resources. The leveraging of external partners involves acquiring pre-built AI solutions or services from vendors, which can enable rapid deployment but potentially can also limit customization, data sovereignty and comes at the risk of vendor lock-in. Finally, the *hybrid model* combines both, where organizations might build some of the models while using external services for commodity and faster value realisation.

All while organizations must navigate an increasingly complex regulatory landscape and maintain their competitive edge.

Our findings emphasize how data governance, compliance, and risk management are becoming foundational elements that help organizations deploy AI responsibly, ensuring ethical standards and security are maintained in an increasingly complex landscape.

The insights provide a clearer picture of how different sectors are adapting to these demands and what best practices are beginning to emerge.

Strategic Insights & Summary

AI Applications & Challenges

3 Trends

Organizations are prioritizing **Data Governance.**

LLMs Leads as primary AI technology.

Predictive Analytics & Automation leads in production.

3 Challenges

Integration with Existing Systems

Shortage of Skilled Expertise

Regulatory & Compliance Pressure

Three Actionable Recommendations

Organizations are prioritizing practical AI deployment over experimentation. While 77% adopt LLMs for rapid value, the real barriers are organizational: expertise gaps, infrastructure limitations, and integration complexity consistently block progress.

Frameworks for Data Governance

Implement solid data principles, version control, and access policies from day one.

- F.A.I.R. Principles in Data for AI - Hopsworks
- Architecture fundamental - Google Cloud Well-Architected Frameworks
- Data Contracts - Principles of Data Economy

Build MVP-First Systems

Deploy production-like environment gradually to test for compliance, security, and integration readiness.

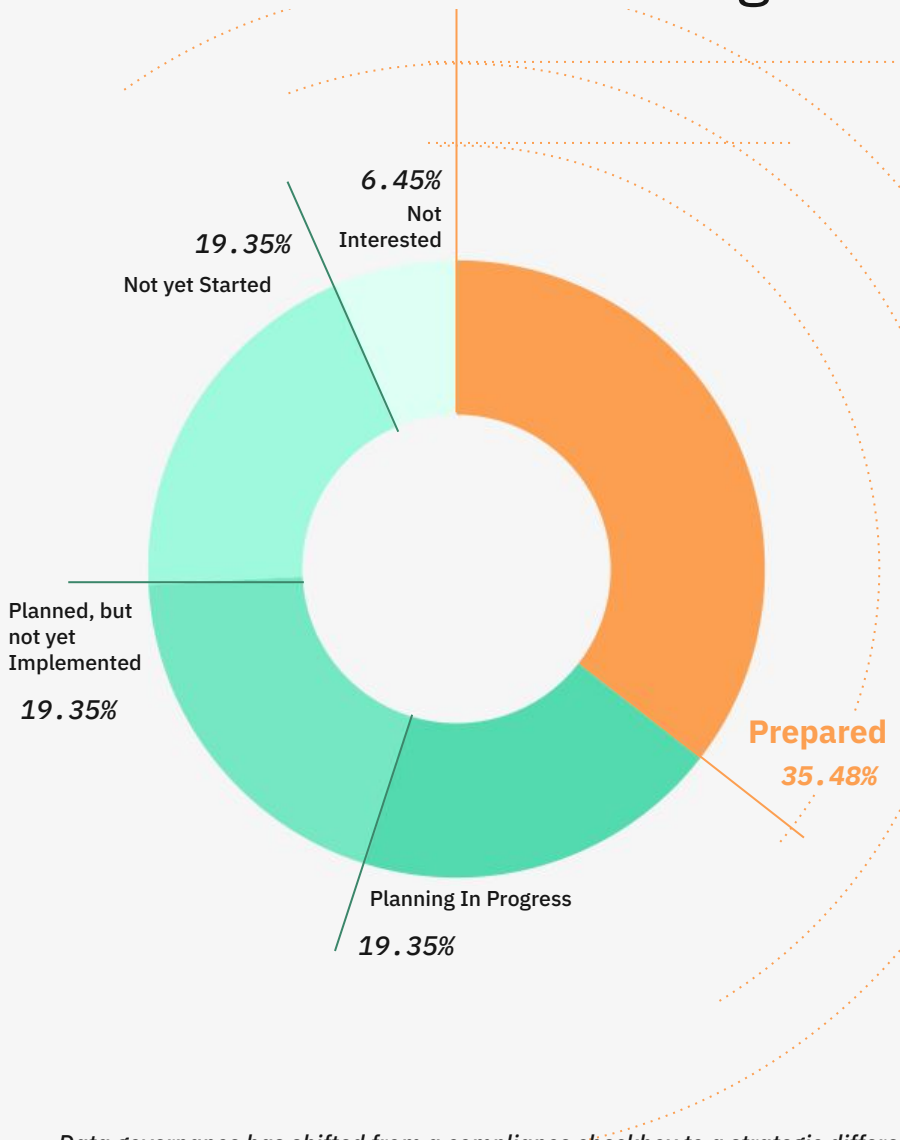
- Continuous Delivery for Machine Learning
- From MLOps to ML Systems with Feature/Training/Inference Pipelines - Hopsworks
- What is a Data Science MVP?

Open Frameworks to Close the Skill Gaps

Reduce expertise barriers by leveraging existing, established and open-source frameworks and tooling.

- The state of open source and rise of AI in 2023 - The GitHub Blog
- Modularity and Composability for AI Systems with AI Pipelines and Shared Storage - Hopsworks

How Prepared are Organizations in Implementing Data Governance Strategies for Sovereign AI?



As Sovereign AI becomes a critical factor of responsible AI development, practitioners and organizations are recognizing the importance of implementing comprehensive data governance strategies. These strategies are essential not only to ensure regulatory compliance and data security but also to uphold ethical standards in the collection, management, and use of data.

However, survey responses reveal a spectrum of maturity levels across organizations, reflecting fragmented progress in adopting these governance frameworks.

The data highlights these varying states of readiness, underscoring the challenges and opportunities that lie ahead for organizations striving to operationalize Sovereign AI responsibly.

Data governance has shifted from a compliance checkbox to a strategic differentiator.

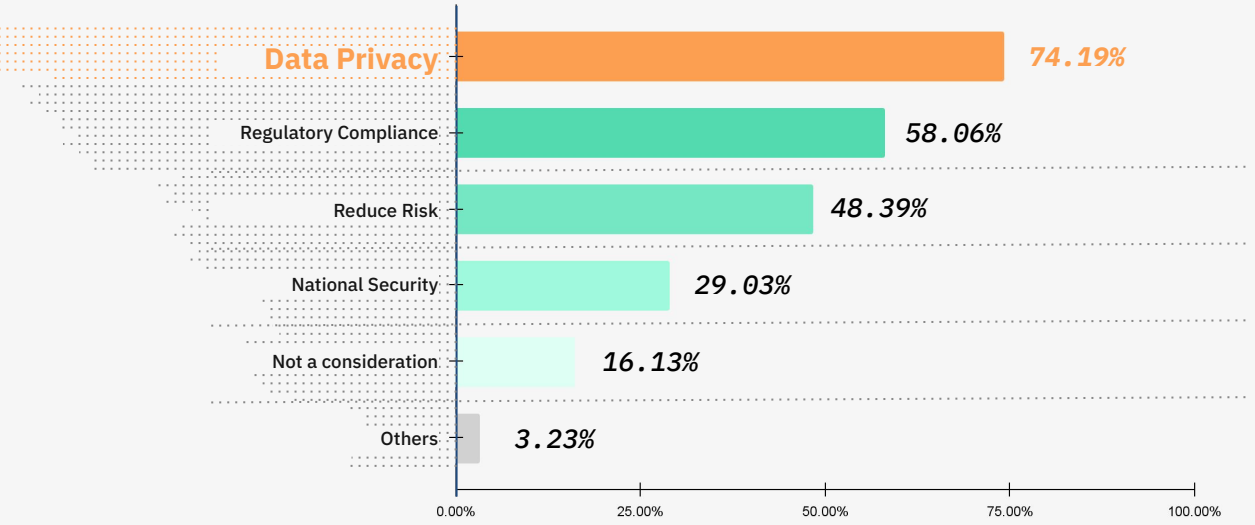
35.48% of organizations have documented data governance frameworks, but only 19.35% have fully implemented them in production systems.

Implementing robust data governance frameworks is essential to ensure data privacy, security, and ethical use, all of which are critical to building trustworthy AI systems. The relatively moderate adoption rate may be due to challenges such as resource constraints, evolving regulatory environments, and the complexity of integrating governance practices into existing data infrastructures. Ultimately, building trust in AI begins with responsible data stewardship.

What are the Main Reasons Behind Adopting Sovereign AI?

With AI becoming increasingly embedded in national infrastructure, enterprise operations, and public services, the concept of **Sovereign AI has emerged as a strategic priority for many countries**. Organizations now see the value in retaining full control over AI systems and infrastructure within their own borders to safeguard sensitive data and critical operations.

Our findings reveal a combination of practical, regulatory, and strategic considerations driving the adoption of Sovereign AI strategies. From ensuring compliance and protecting critical data to strengthening operational resilience and national autonomy, these interconnected factors are shaping how organizations approach AI integration in the era of digital sovereignty.



*Note: As multiple selections were allowed, percentages correspond to the share of total participants choosing each answer, **which results in totals exceeding 100%.**

Over 74% of respondents prioritize Data Privacy as the main driver for Sovereign AI adoption.

About 50% of respondents identified Regulatory Compliance and Risk Reduction as key secondary factors stressing also the importance of ensuring AI systems align with evolving legal and security frameworks to stay compliant in a rapidly changing regulatory landscape.

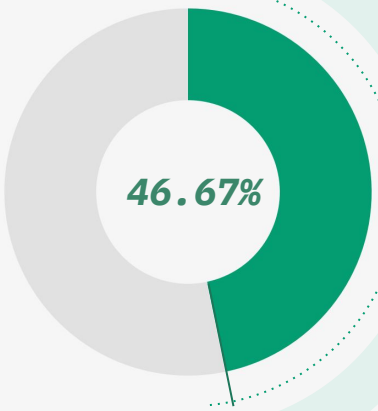
Interestingly, ***16.13%*** of respondents indicated that Sovereign AI is not a consideration, which may suggest either a lack of awareness, perceived low risk, or heavy reliance on global AI providers.

While the primary motivations for Sovereign AI are rooted in privacy and compliance as the survey results depict, the broader narrative includes risk mitigation, control, national interests and scaling to an extent. As AI governance matures, Sovereign AI will likely become a strategic imperative, not just be limited to a technical choice.

Which Approach are Organizations Currently Following for AI Models?

Organizations are leveraging AI to drive innovation and optimize operations, and their approach to developing AI models varies. The survey results highlight the strategies employed by organizations, revealing a balance between in-house development, external providers, and hybrid approaches in navigating AI adoption.

Build your Own Models Approach



Nearly 46.67% indicated that their organizations focus on building their own AI models.

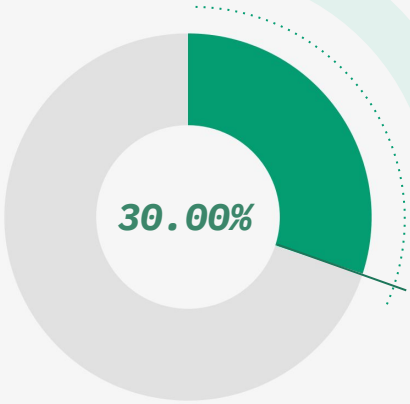
Reflecting a dominant strategic commitment to full-stack control over AI development, from data sourcing and model architecture to deployment and governance. Organizations choosing this route often seek to tailor AI systems to their specific operational needs, ensure compliance with internal security standards, and retain intellectual property.

Around 30% get their AI models from external sources to simplify and streamline implementation.

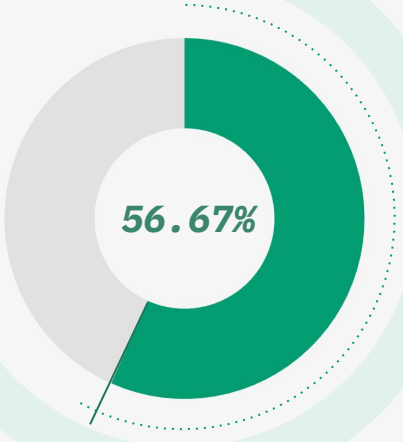
Allowing organizations to accelerate adoption by leveraging pre-built solutions from established vendors, reducing the need for internal development capacity.

Early-stage AI adopters typically prefer buying external solutions, given the speed and practicality it offers. It also minimizes upfront investment, access cutting-edge capabilities quickly, or operate without extensive in-house AI expertise.

Buy from External Providers Approach



Use Hybrid AI Model Approach



56.67% of organizations use a hybrid approach, integrating both internal development & external resources.

Leveraging the best of both worlds; a dual approach, enabling them to customize and control their AI assets, increase operational efficiency, reduce risks, and quickly adapt to the rapidly evolving technological advancements and scalability offered by external vendors.

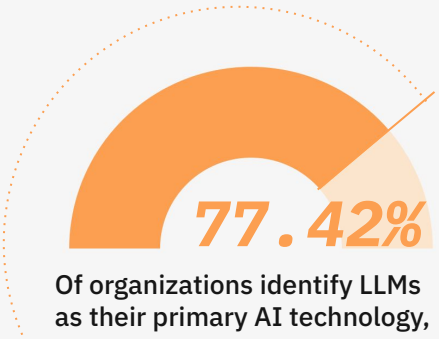
Organizations are strategically choosing between building, buying, or combining AI solutions to balance customization, speed, and resource optimization. This flexible approach enables them to address unique operational needs while staying agile in a rapidly evolving technological landscape.

*Note: As multiple selections were allowed, percentages correspond to the share of total participants choosing each answer, which can result in totals exceeding 100%.

How are Organizations Applying AI Models in Practice?

From task automation to advanced language models, the types of models chosen reflect both technological maturity and strategic priorities. This survey reveals which model types are currently in use across different organizations.

Organizations with LLM as their Leading AI Model



Of organizations identify LLMs as their primary AI technology,

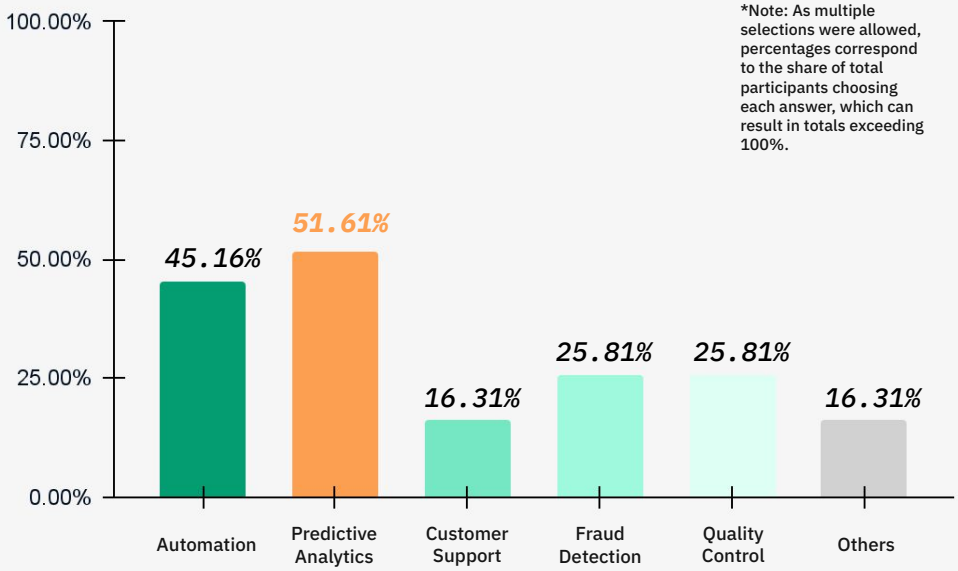
LLMs are massively favored across many organizations; for their ability to handle tasks like language understanding and content generation.

"LLMs ability to deliver a fast user experiences, is likely what's making them practitioners' leading types of models for initial implementation."
Lex Avstreikh, head of strategy at Hopsworks

Organizations have Moved Beyond AI Experimentation

to focus on applications with clear, measurable impact. The emphasis on **automation** and **predictive analytics** reflects a practical approach, these technologies deliver immediate operational benefits while providing the foundation for more advanced AI implementations.

Actual production use cases remain focused on traditional applications: automation 45.16% & predictive analytics 51.61%.



*Note: As multiple selections were allowed, percentages correspond to the share of total participants choosing each answer, which can result in totals exceeding 100%.

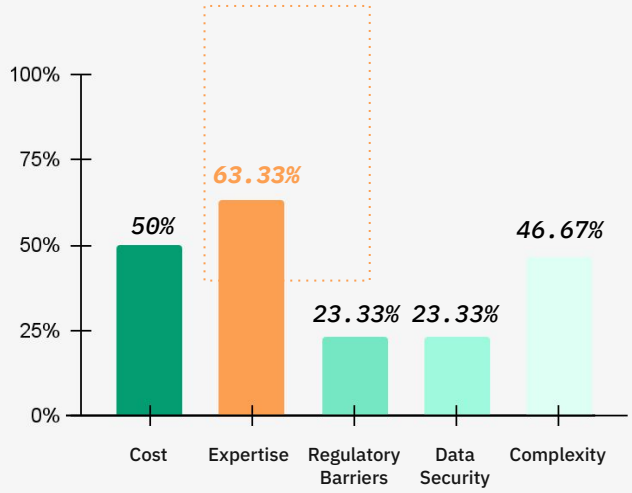
A clear pattern; companies prioritize AI that either saves money or prevents disasters. LLMs win because of their plug-and-play nature, allowing for powerful and fast value visibility. Predictive analytics and fraud detection offer quantifiable protection against risk. Customer-facing AI remains secondary, organizations are securing their operations first, then enhancing customer experience and providing AIs that are customer facing.

What Challenges do Organizations Face in Implementing Sovereign AI?

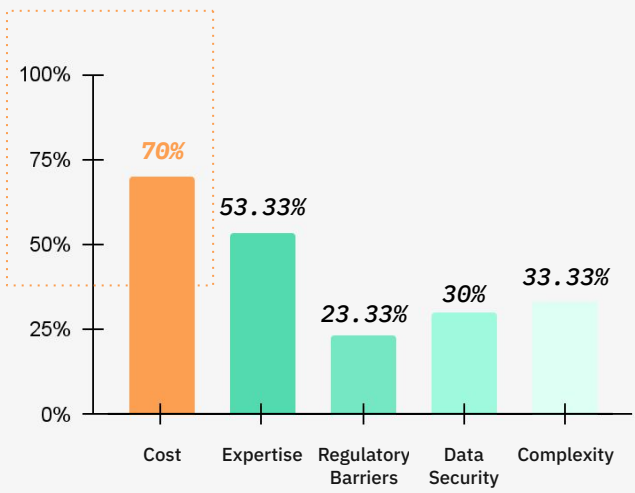
Implementing Sovereign AI presents a range of challenges, spanning from infrastructure development to data security and regulatory compliance.

This question explores the critical obstacles organizations encounter throughout their Sovereign AI journey. The following analysis focuses on five key areas where these challenges are most pronounced, highlighting the barriers faced by organizations opting to develop solutions internally.

For Building the Processes



For Building the Infrastructure



*Note: As multiple selections were allowed, percentages correspond to the share of total participants choosing each answer, which can result in totals exceeding 100%.

Three major barriers dominate AI implementation:

Expertise shortages 63.33%, high costs 50% & system complexity 46.67%.

Regulatory and security concerns also add layers of difficulty.

Costs dominate infrastructure challenges at 70%, but the expertise gap (53%) reveals a deeper issue.

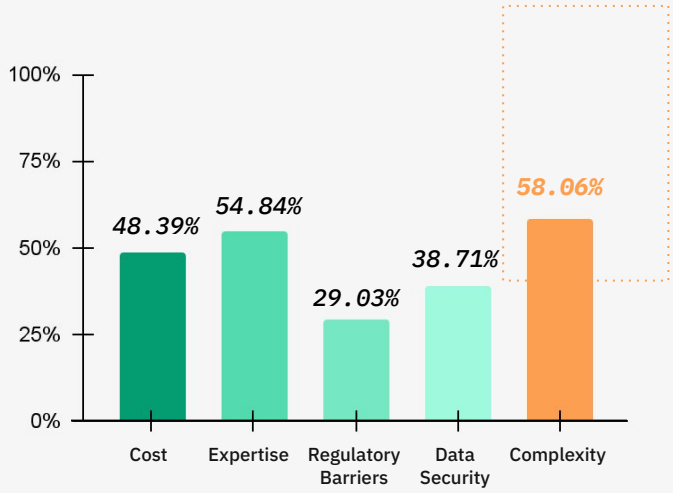
Organizations lack the skilled teams needed to build effective Sovereign AI systems.

To successfully build Sovereign AI, organizations must focus on AI expertise and simplifying process complexity while ensuring sufficient budget allocation for infrastructure. Additionally, ensuring compliance and safeguarding data are vital throughout the AI development phase.

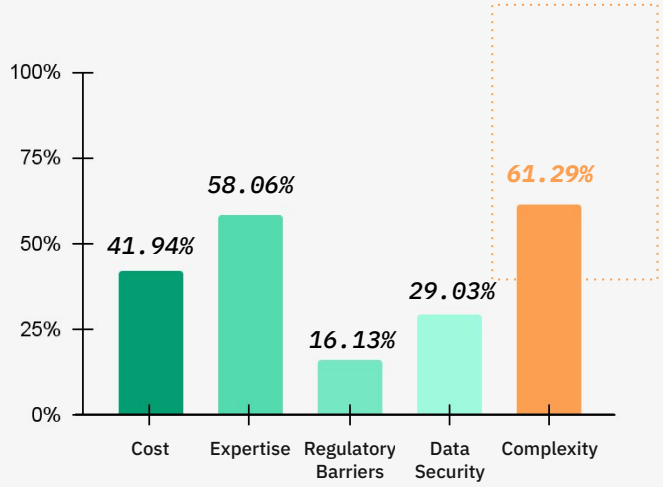
What Challenges do Organizations Face in Implementing Sovereign AI?

This section examines the key challenges organizations face when integrating Sovereign AI into existing systems and processes. From aligning with current IT infrastructure to adapting data workflows and management practices, integration emerges as a critical hurdle in operationalizing AI at scale. These challenges underscore the need for strategic planning, cross-functional collaboration, and scalable architectures to ensure seamless AI integration across the enterprise.

For Integrating it with Existing Data Sources and Workflows



For Integrating with Existing IT Infrastructure



*Note: As multiple selections were allowed, percentages correspond to the share of total participants choosing each answer, which can result in totals exceeding 100%.

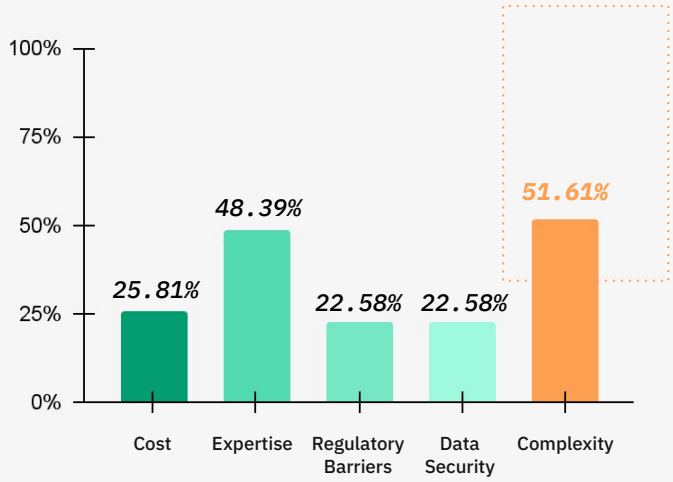
Sovereign AI integration faces a consistent challenge pattern regardless of focus area. Whether organizations are connecting to existing data sources or IT infrastructure, the same three barriers dominate:

Complexity (58-61%), Expertise shortages (55-58%), Cost (42-48%).

Integration isn't optional, it's make-or-break for AI success. Organizations that fail to align AI capabilities with existing systems face performance bottlenecks, compliance failures, and wasted investments. The challenge goes beyond technical compatibility to encompass governance frameworks, data workflows, and operational processes that determine whether AI delivers value or becomes an expensive distraction.

What Challenges do Organizations Face in Implementing Sovereign AI?

Integrating with Existing Management Processes



*Note: As multiple selections were allowed, percentages correspond to the share of total participants choosing each answer, which can result in totals exceeding 100%.

Complexity 51.61% and expertise shortages 48.39% are again most commonly faced.

In contrast, cost, regulatory barriers, and data security, each cited by fewer than 26%, appear to be secondary concerns, indicating that internal readiness is the primary hurdle organizations must overcome.

Across all stages of Sovereign AI implementation, whether building infrastructure and processes or integrating with existing systems; complexity, high cost & expertise shortages consistently emerge as the primary challenges.

Here we see a clear pattern: from the practitioner's perspective Sovereign AI and implementation of AI systems success hinges on organizational readiness.

The real barrier isn't building Models, it's building the expertise, processes, and culture to deploy it effectively at scale.

2 Section:

AI Governance, Security & Future Strategy

Section Overview

Organizations are aligning their AI initiatives with governance, security, and strategic foresight to ensure responsible and scalable deployment:

AI Governance:

Push to establish robust governance frameworks that ensure **ethical AI use**, **regulatory adherence**, and **transparent accountability**. These frameworks are essential to mitigate risks such as algorithmic bias, misuse, and non-compliance. (see **F.A.I.R principles** in Machine Learning)

Security and Data Control:

As more AI workloads and sensitive data are processed through external models or hybrid infrastructures, organizations are prioritizing data protection. Ensuring data sovereignty, secure model interactions, and privacy-by-design are becoming central to enterprise AI strategies.

Future Strategy:

Long-term AI success depends on cohesive strategies that align governance and security with organizational goals. This includes developing internal capabilities, investing in secure infrastructure, and adopting Sovereign AI principles to maintain autonomy and trust.

These pillars support sustainable AI maturity, enabling organizations to innovate while safeguarding integrity and public trust.

What follows are insights on how organizations are enhancing AI governance, tackling security and data sovereignty challenges and plans for future AI strategies.

Strategic Insights & Summary

AI Governance, Security & Future Strategy

3 Trends

74% prioritize
Data Privacy
as #1 driver

Growing trend of
Combining On-premises & Cloud

Emphasis on
Compliance & Audit Processes

3 Challenges

Balancing Security with Cost Control

Data Quality & Integrity
Difficult to maintain across systems

Bias & Ethical Risks
Ranked lower but growing concern.

Three Actionable Recommendations

69% of organizations view Sovereign AI as essential to their strategy. Organizations that embed controls early will position themselves to navigate regulations while maintaining innovation velocity.

Scalable AI Infrastructure

Build infrastructure that handles millions of predictions daily.

- Hidden Technical Debt in Machine Learning Systems
- Meet Michelangelo: Uber's Machine Learning Platform | Uber Blog
- The Hopsworks Feature Store for Machine Learning | International Conference on Management of Data

Multi-layered Security Protocols

AI systems with security at every layer: data, model, & infrastructure

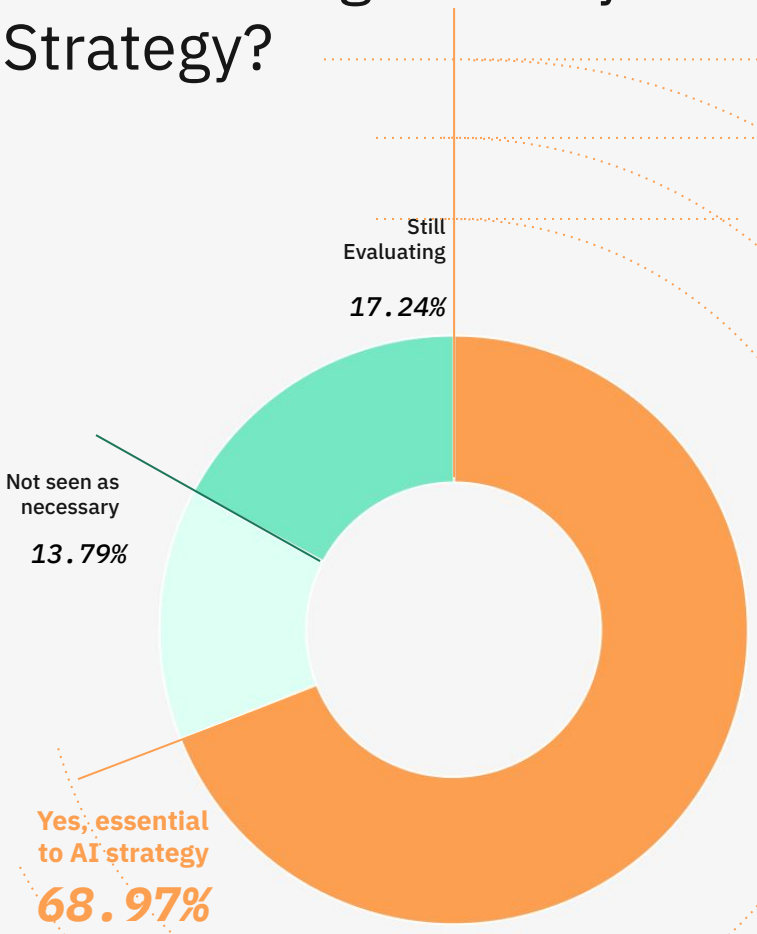
- What is Zero Trust Architecture? - Palo Alto Networks
- Part 1: Privacy Preserving Machine Learning: Encryption for the Rest of Us — Data for the Best of Us
- How we secure your data with Hopsworks

Internal Policies & Data Principles

Embing governance in your engineering frameworks.

- Responsible Generative AI Toolkit | Google AI for Developers
- Artificial Intelligence Risk Management Framework
- Google use case: Responsible AI Progress Report

Will Sovereign AI Play a Pivotal Role in Enterprise Strategy?



Today, many organizations are reassessing how to **build trust, accountability, and control into their systems with increased AI adoption**. Amid evolving global regulations and increasing scrutiny over data usage and model transparency, Sovereign AI is emerging as a key pillar of responsible innovation.

More than just a compliance requirement, it represents a strategic shift, enabling enterprises to retain autonomy over their infrastructure, safeguard sensitive data, and align AI development with national and organizational priorities.

With the rise of regulations like the EU AI Act, organizations are turning to Sovereign AI to ensure compliance while maintaining control over their data and AI systems.

By integrating Sovereign AI into their strategies, organizations hope to secure a competitive edge in an increasingly complex digital landscape.

Only a small portion ***around 14%*** do not currently see Sovereign AI as a key factor, suggesting limited but notable skepticism or differing priorities among a minority.

68.97% of organizations anticipate Sovereign AI will play a pivotal role in their AI strategies over the next half decade. This Signals a strong shift toward responsible AI practices and enhanced control over AI systems and data.

Top Data Governance Priorities When Using External LLMs, ML Models or Infrastructure

As reliance increases on external large language models (LLMs), machine learning models, and related infrastructure, effective data governance becomes paramount. Understanding and prioritizing key concerns helps organizations safeguard their AI deployments while maximizing value.

We asked respondents to rank **six critical governance concerns** related to the use of external large language models (LLMs), machine learning models, and infrastructure.

This ranking provides valuable insights into the factors shaping policy development, risk management strategies, and investment decisions in the evolving AI landscape.

The results show that data privacy 4.86 ranked highest among data governance priorities, followed by data quality 3.93, and model reliability 3.71,

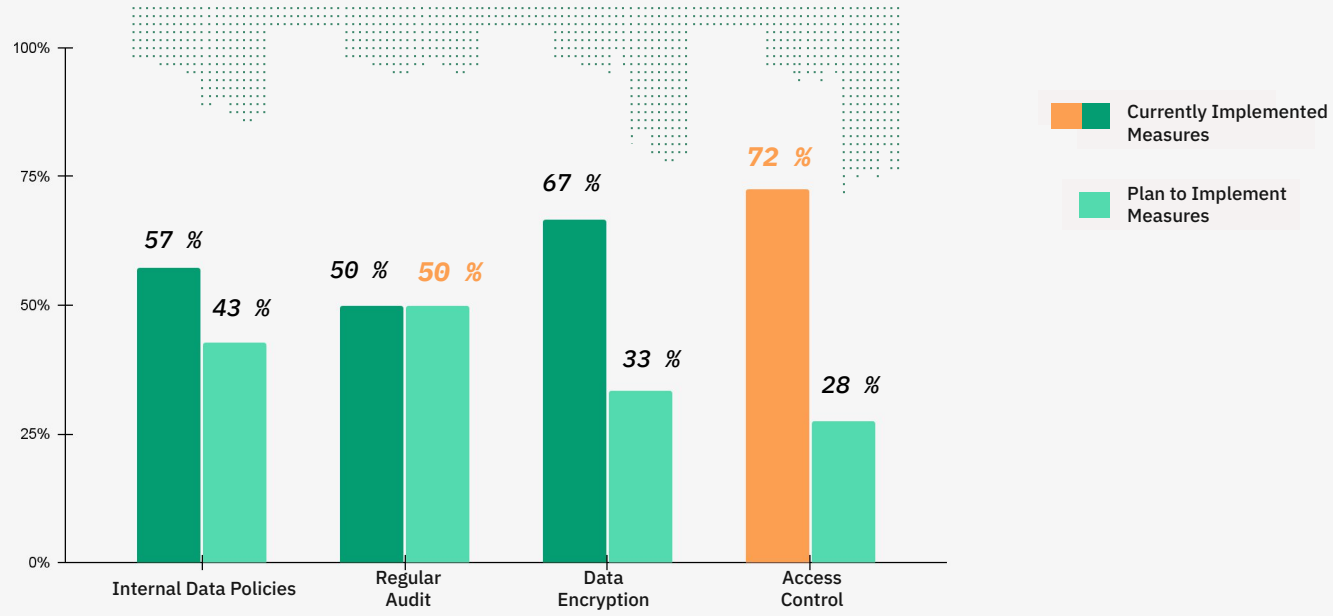
This indicates that organizations currently view trust, control, and consistent performance as the foundations of responsible external AI adoption.

Scalability, cost management, and ethical risks remain secondary concerns, suggesting they are emerging priorities rather than immediate challenges. As organizations work to establish foundational trust and performance in external AI use, these areas may grow in importance as adoption scales and systems become more complex.

Attention is centered on getting the fundamentals right, particularly around data and model integrity, before expanding governance efforts. As maturity increases, we expect a natural progression toward addressing deeper ethical and systemic risks through more comprehensive tooling and oversight.

What are the Current & Planned Data Governance Measures for Sovereign AI?

For businesses working on advancing their Sovereign AI capabilities and the shift toward structured data governance this insights reflects growing regulatory awareness and efforts to mitigate risk and maintain trust . By implementing controls early, organizations ensure compliance and build trust, enhance operational efficiency, & can position themselves competitively in markets.



Access control 72.41% & data encryption 66.67% are the most commonly implemented practices. This reflects that the initial implementation steps, are foundational security measures that provide immediate protection and demonstrate clear value to stakeholders; safeguarding data through technical and infrastructure-level controls.

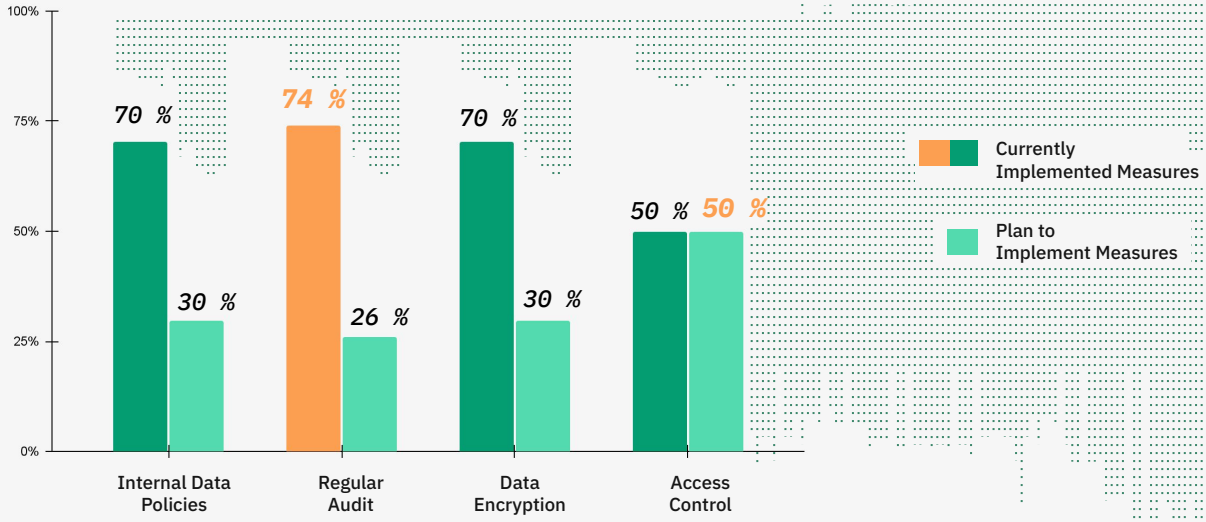
42.86% of organizations plan to introduce internal data policies, signaling a shift toward comprehensive governance frameworks as Sovereign AI initiatives mature beyond initial technical implementations.

As Sovereign AI initiatives scale in complexity and scope, organizations that embed these controls early will be better equipped to navigate regulatory requirements, minimize risk exposure, and establish long-term stakeholder confidence and trust.

What are the Current Sovereign AI Adopted Practices?

With growing geopolitical tensions and stricter data localization laws, AI data sovereignty is just **no longer solely a compliance requirement but a strategic one** for all organizations leading to data sovereignty becoming a defining factor in AI strategy. Organizations are adopting a range of technical and policy-driven measures to ensure that sensitive data remains secure, compliant, and under appropriate jurisdictional control.

This question explores how enterprises are addressing AI data sovereignty through their infrastructure, security practices, and regulatory safeguards.



With regional cloud providers, on-premises storage and encryption all around the 70% mark,

it is evident that those are emerging as the most commonly implemented approaches, highlighting a strong preference for localized control.

Planned adoption of compliance audits by 50% of organizations indicates a slowly growing awareness of the need for structured and ongoing mechanisms.

This multi-faceted approach signals a strategic balance between safeguarding sensitive information, meeting regulatory standards, and enabling flexible, secure AI operations across diverse jurisdictions.

3 Section:

AI Infrastructure & Readiness

Section Overview

AI Infrastructure and Readiness require more than just selecting the right technologies, whether cloud, on-premises, or hybrid environments, to handle AI workloads efficiently.

Organizations must ensure their infrastructure offers the right balance of flexibility, scalability, security, control, and cost-effectiveness to support complex AI operations. Equally important is assessing whether the current infrastructure can meet these demands, as AI workloads **often require specialized computing power and optimized data management**.

Equally critical is organizational readiness. Companies must align skills, processes, and governance frameworks to support sustainable AI deployment. Together, infrastructure and readiness form the foundation for reliable, compliant, and high-performing AI systems at scale.

Here we are addressing essential considerations through key questions about current infrastructure capabilities, preferred data infrastructure types, foundational components for Sovereign AI stacks, and integration challenges.

This section examines how leading organizations are building AI-ready infrastructure, the critical gaps that derail implementation, and the strategic moves that separate successful deployments from costly failures.

Strategic Insights & Summary

AI Infrastructure & Readiness

3 Trends

Trend towards enabling rapid data processing & ***Faster or Real-time Use Cases.***

Custom models & open-source frameworks ***Drive AI Sovereignty***

organizations prefer ***Cloud-based Platforms*** as they are de facto ready platforms.

3 Challenges

Quality issues impacting ***Accuracy & Reliability***

Fragmented Data Access

Legacy Systems Limitations

Three Actionable Recommendations

With 46% of organizations lacking adequate AI infrastructure, success requires pragmatism: governance first, MVP deployment, then scale with open frameworks. This builds real operational capabilities at scale.

Organisational Readiness

Assess risks early, define clear use cases before scaling.

- The 10 Fallacies of MLOps - Hopsworks
- What is the business problem that we are trying to solve here?
- Rules of Machine Learning: | Google for Developers

Modernize AI Infra Foundations

Build on unified data storage, open table format, and abstractions allowing reusable data and engineering pipelines.

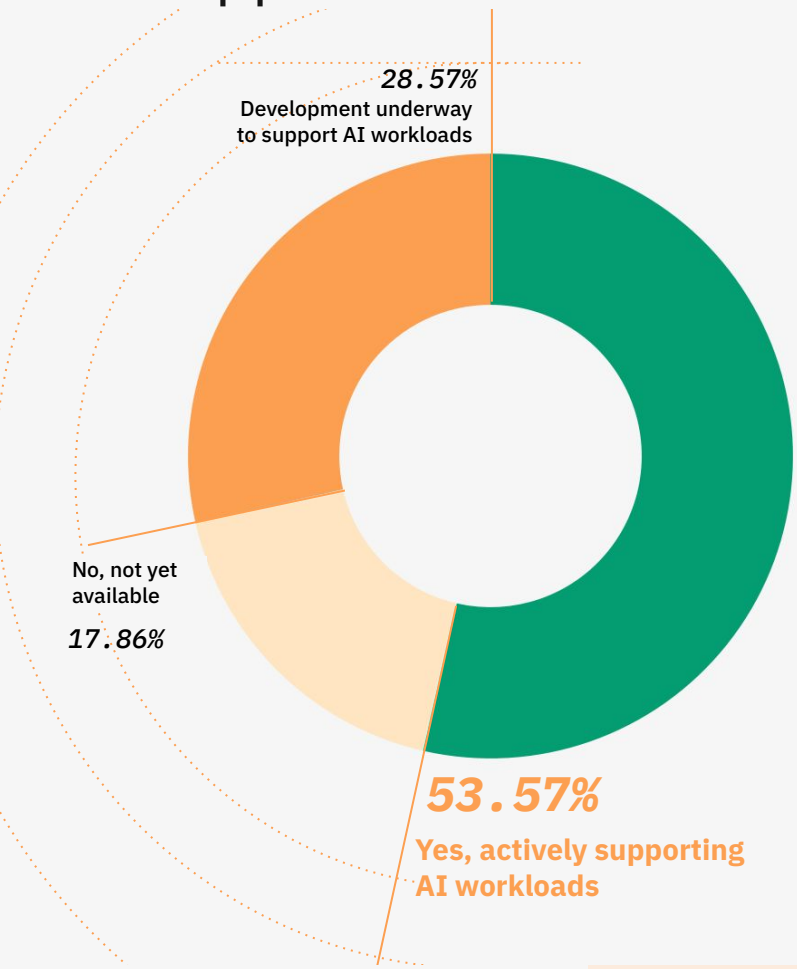
- The Architect's Guide to Open Table Formats and Object Storage - The New Stack
- What is a Feature Store: The Definitive Guide - Hopsworks

Modularity & Compatibility

Build with existing system using interoperable technologies and principles

- The Taxonomy for Data Transformations in AI Systems - Hopsworks
- Modularity and Composability for AI Systems with AI Pipelines and Shared Storage - Hopsworks

Does your Organization Have Infrastructure to Support AI Workloads?



Establishing resilient and scalable infrastructure is critical for maintaining secure and efficient AI processes.

An organization's ability to support AI workloads spanning from computing power, storage capacity, to seamless data integration serves as a clear indicator of its overall AI maturity.

Effective AI infrastructure enables efficient development, deployment and monitoring of AI system., and supports iterative model training and deployment without bottlenecks.

A cumulative 46.43%, nearly half of the respondents, report that they do not currently possess the technical foundation needed to scale AI capabilities.

Only 53.57% of organizations have access to AI-capable compute resources, with the majority (estimated 40%+) relying entirely on managed cloud services rather than sovereign infrastructure.

It is to note that previous surveys in the field such as the **Economist Impact study conducted in 2024** had found that figure to **be below 30%.** While it is likely that many organization have undergone aggressive implementation of infrastructure it is much more likely that they preferred simpler implementation to catch the gap.

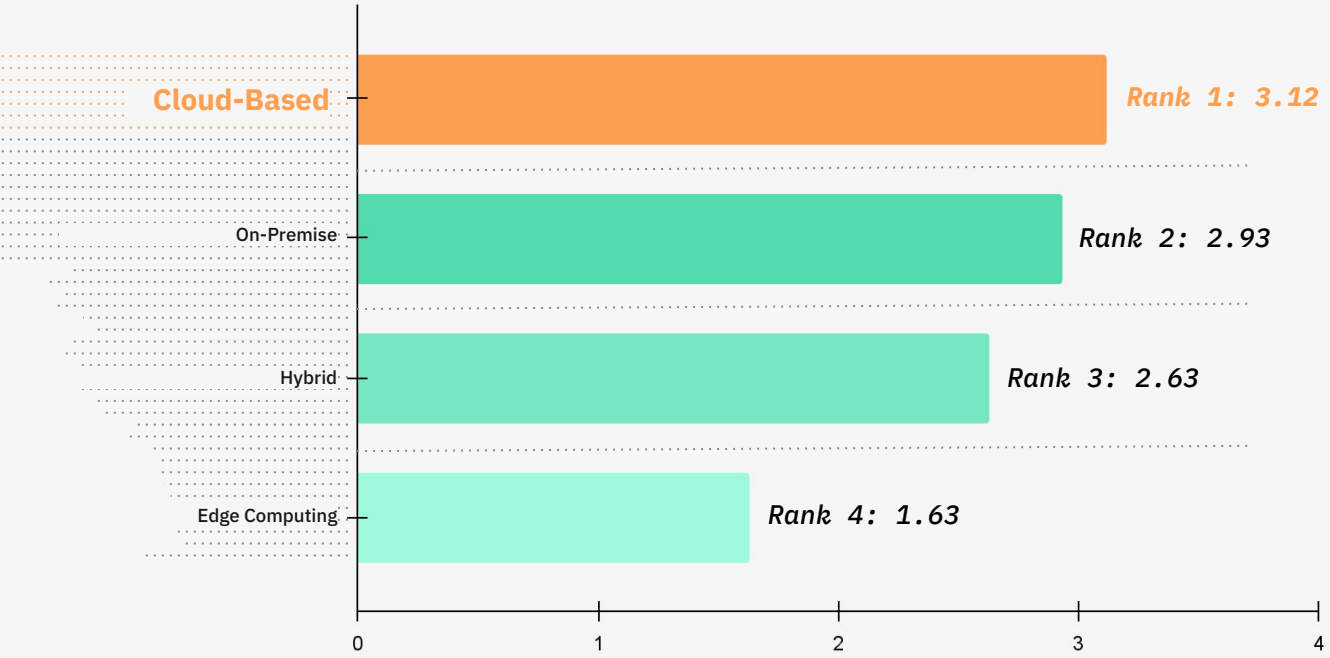
Answers in our survey also suggest that infrastructure for LLMs and more classic machine learning use cases are often interchangeably used to describe AI infrastructure, blurring further the line between the actual organizational capability and the ability to use an LLM.

This deficit of infrastructural knowledge and the actual gap represents a significant strategic challenge for organizations pursuing Sovereign AI initiatives. Without robust foundational capabilities, organizations currently relying on external cloud infrastructure must carefully evaluate whether their existing arrangements provide sufficient governance mechanisms and data residency controls.

Which AI Data Infrastructure are Organizations Prioritizing?

Organizations are embracing diverse data infrastructure models to meet evolving demands around performance, security, and compliance. These infrastructure choices are being strategically aligned with business objectives, playing a critical role in shaping AI capabilities and supporting long-term goals.

To better understand the key priorities influencing these decisions, we asked respondents to rank four core data infrastructure strategies. Their responses offer valuable insight into the factors driving model selection and the growing adoption of flexible, purpose-driven data architectures.



At 3.12, Cloud-based infrastructure unsurprisingly emerged as the top choice among organizations.

Highlighting its importance in delivering easily scalable, flexible, and tool-rich environments essential for AI development.

This preference reflects a state where agility and rapid innovation is necessary.

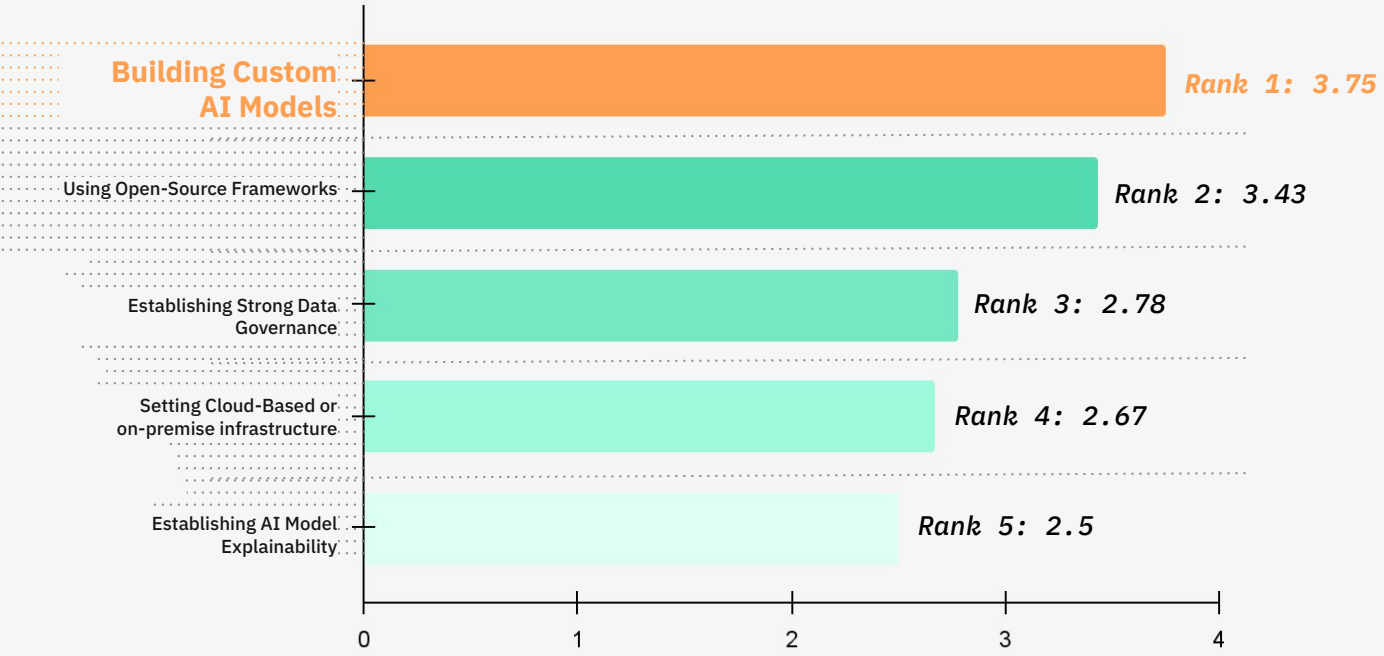
On-premise and hybrid infrastructure are showing growth—solutions that were once preferred primarily for specific legal considerations or by traditionally conservative businesses are emerging as viable options across many organizations, particularly among those prioritizing data control, security, or regulatory compliance, where full cloud adoption may not be feasible.

Additionally, with the commoditization of the infrastructure layer and its hardware, full infrastructure control becomes more accessible for smaller organizations, especially where cost considerations are important.

Strategic Considerations for Developing a Sovereign AI Stack

Organizations are increasingly focused on building technology stacks that ensure full control, autonomy, and minimize reliance on external providers. To identify which elements are most critical to an effective Sovereign AI strategy, we asked respondents to rank five key components by their priority.

Their responses provide insights into the approaches currently seen as most effective for achieving data independence and control while developing Sovereign AI infrastructures.



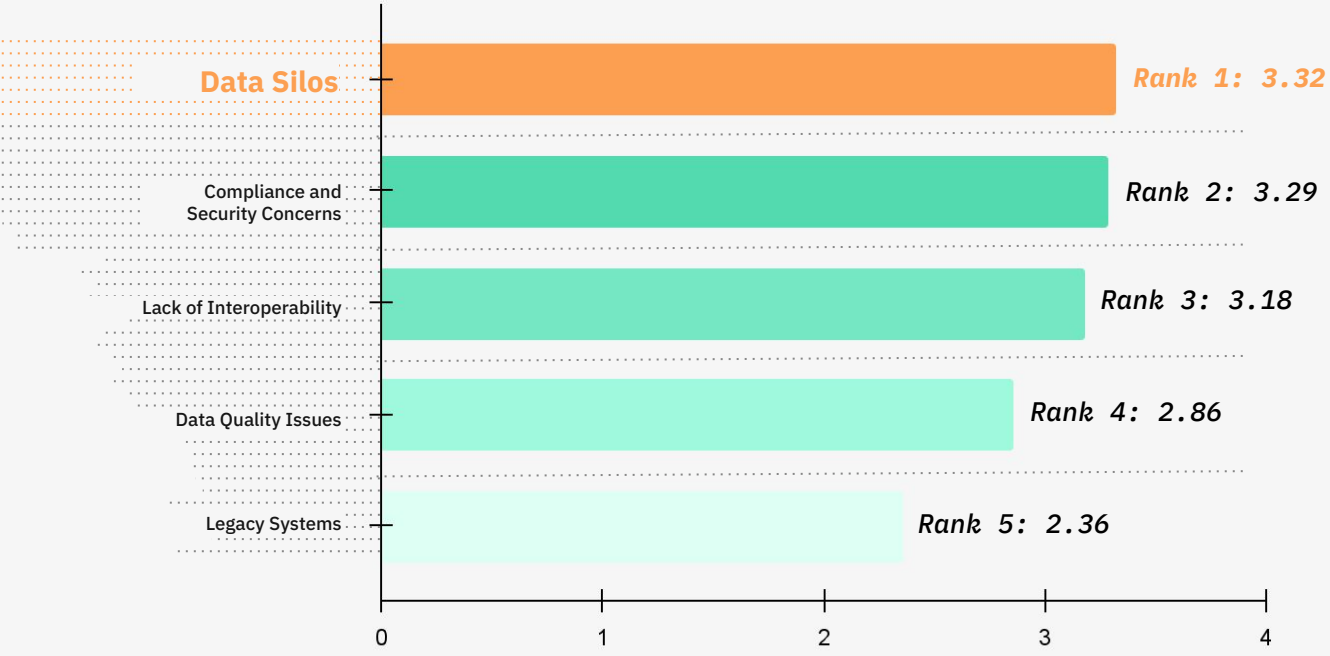
Building Custom AI models with open-source Frameworks are the top priority for organizations aiming to build Sovereign AI stacks.

This signals a motivation to shift away from one-size-fits-all approaches, as enterprises seek to differentiate themselves through proprietary AI capabilities that reflect their unique operational contexts..

Organizations also highlighted the importance of model lifecycle management and version control for end-to-end traceability, from training to deployment and rollback. This focus points to required best practice and operational necessity when AI systems mature and the need for governance, auditability, and operational resilience increases.

Main Hurdles Faced by Organizations While Integrating Data Across Different Systems.

Successful implementation of a Sovereign AI strategy depends heavily on seamless data integration across diverse systems. To better understand the main roadblocks, we asked organizations to rank five common integration hurdles and the findings below show the current struggles faced by them..



Data Silos is the topmost hurdle faced with score 3.32 by organizations when building scalable AI systems.

This highlights a persistent and fundamental challenge to integrate and access datasets across departments, infrastructures and platforms.

Compliance and security concerns 3.29 rank second, showcasing a rising focus on data governance amid tighter regulations and growing use of sensitive data in AI.

While the lack of interoperability remains a key challenge in unifying AI systems, concerns around data quality appear to be easing, and legacy systems are seen as less problematic while still posing risks if not modernized. Even though, organizations are making progress on foundational data challenges, but seamless **integration and future-ready infrastructure remain critical for scalable AI success.**

Other responses and key hurdles that organizations face include **inconsistent metadata, real-time data constraints, and difficulties enforcing scalable governance in Sovereign AI environments** as well as resistance from management and funding constraints in Sovereign AI environments.

HOPSWORKS

THANK YOU

Deploy your own Sovereign AI

Try Hopsworks for Free

Sovereign AI Solutions by Hopsworks

public-hopsworks.slack.com